TECNOLOGIAS WEB: Seguridad en tecnologías web

3º Grado en Ingeniería Informática
Especialidad Tecnologías de la Información

Germán Martínez Maldonado
germanm@correo.ugr.es

Introducción

El objetivo de este trabajo es hacernos una idea de la importancia que tiene la seguridad en el ámbito de los sistemas informáticos, y sobre todo cuando nos referimos a la Web, por este motivo vamos a hacer una lista con los incidentes de seguridad más frecuentes que se dan en el ámbito de las tecnologías web, ya sea en la redes, servidores o aplicaciones; realizando además una pequeño descripción sobre los mismos.

Problemas

A la hora de pensar en cómo estructurar la seguridad de una red hay varios aspectos básicos que deberíamos tener en cuenta:

- **Confidencialidad:** toda información debe estar protegida de accesos no autorizados, solo podrá ser accedida por los medios autorizados.
- **Integridad:** toda información debe estar protegida de modificaciones no autorizadas, la información debe tener la misma exactitud que cuando fue generada.
- **Disponibilidad:** toda información debe estar disponible para cualquier medio autorizado, en cualquier momento que sea requerida.
- **Autenticación:** toda información debe tener inequívocamente un origen legítimo controlable y demostrable, para que un tercero no pueda suplantarlo.

Para cubrir con todos estos posibles inconvenientes podremos utilizar diferentes sistemas de filtrado de tráfico, protección criptográfica, sistemas de copias de seguridad y gestión de cuentas de usuario.

Los problemas descritos irían más enfocados a la protección de la información en la redes, pero también deberemos tener en cuenta otro aspecto importante como es la seguridad en la conexiones con las redes, sobretodo en redes inalámbricas, ya que realizarse la transmisión por un solo canal guiado, la información que circula por ella es muy susceptible de ser interceptada, es por eso que deberemos tener en cuenta medidas de seguridad como utilizar sistemas de cifrados WEP o WPA o sistemas de filtrado según la dirección MAC.

Los servidores web son los elementos que tienen una mayor exposición ante un ataque, ya que son los que dan el servicio a la web, por eso deberemos tener en cuenta su configuración para cubrir todas las posibles vulnerabilidades que hayan sido descubiertas, ya vayan desde la manipulación de URL para provocar situaciones inesperadas, aprovechamiento de fallos en sistemas de identificación o inyección de código maligno.

Pero ya no solo en el aspecto de configuración de los servidores deberemos centrarnos, ya que también es posible protegerlos en gran medida mediante el uso de cortafuegos, pudiendo optar desde simples cortafuegos que únicamente se encargan de realizar un filtrado básico en el tráfico manejado a, otros sistemas más sofisticados, que nos darán funcionalidades extras

desde el tipo cortafuego de aplicaciones, balanceo de carga o hasta bloqueo de amenazas software como inyección de código o ataques por desbordamiento de buffer.

Ya en las aplicaciones web, nos encontramos también problemas similares a los ya vistos, como son la validación de datos, la autenticación o el manejo de sesiones. Dentro de la validación de datos, los principales problemas que nos encontramos son:

- **Inyección SQL:** consistente en aprovechar una vulnerabilidad de la aplicación para introducir código malicioso que nos dé acceso a unos campos de la base de datos a los que normalmente no tendríamos acceso.
- **XSS (Cross-site scripting) o secuencias de comandos en sitios cruzados:** consiste en aprovechar una vulnerabilidad como la anterior, pero usando en este caso código en un lenguaje script como JavaScript, pudiendo realizar acciones perjudiciales para un usuario en su propio sistema.
- **Desbordamiento de buffer:** consiste en aprovechar un fallo de programación en el control de la cantidad de datos que se copian en la zona de memoria reservada, esto puede hacer necesario que se almacenen más datos de los estimados originalmente, por lo que puede afectar a zonas de memoria asignadas a otros programas, lo que puede provocar un comportamiento imprevisto en el sistema que puede ser usado por un atacante.

Como problemas a la hora de autenticar podemos encontrarnos sobretodo problemas que son culpa en mayor parte por parte del usuario, como puede ser la falta de una política para la creación de contraseñas o abusar de la opción de “Recordar contraseña”, ya que esto puede facilitar el robo de credenciales mediantes ataques por fuerza bruta u otro tipos de ataques que aprovechen vulnerabilidades con tal fin.

Por último, como problemas en el manejo de sesiones podemos encontrarnos la manipulación de cookies y tokens, que puede producir que la información que se está transmitiendo entre el servidor y el cliente haya sido falseada deliberadamente para sacar provecho de una situación que no se debería producir; también puede ser que nos encontremos con variables de sesiones expuestas, que podría hacer que la información que hayamos introducido en un página web, sea accedida por una tercera persona, quedando nuestra información a su libre disposición para cualquier que sea su interés; o la falsificación de petición de sitios cruzados, que hace que mediante un script malicioso, un sitio web que considera a un usuario como legítimo, realice operaciones no permitidas a través de este último.

Referencias:

Referencias consultadas a 1 de abril de 2013:

Enlace 1: “Seguridad de la información – Wikipedia, la enciclopedia libre”, última modificación 15:55 24/03/2013: http://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n

Enlace 2: “Seguridad en redes de computadoras – Monografias.com”, Juventino Gutiérrez Prieto, 25/01/2007: http://www.monografias.com/trabajos43/seguridad-redes/seguridad-redes.shtml

Enlace 3: “Ataques al servidor Web”, Juventino Gutiérrez Prieto, 04/2013: http://es.kioskea.net/contents/attaques/attaques-web.php3

Enlace 4: “Seguridad en Aplicaciones Web”, Gabriel E. Arellano, 2008: http://www.slideshare.net/aretche/seguridad-de-aplicaciones-web-presentation

Enlace 5: “Inyección SQL – Wikipedia, la enciclopedia libre”, última modificación 23:30 07/03/2013: http://es.wikipedia.org/wiki/Inyecci%C3%B3n_SQL

Enlace 6: “Cross-site scripting – Wikipedia, la enciclopedia libre”, última modificación 23:30 07/03/2013: http://es.wikipedia.org/wiki/Cross-site_scripting

Enlace 7: “Desbordamiento de Buffer – Wikipedia, la enciclopedia libre”, última modificación 12:05 15/03/2013: http://es.wikipedia.org/wiki/Desbordamiento_de_b%C3%BAfer

Enlace 8: “Cookie (informática) – Wikipedia, la enciclopedia libre”, última modificación 14:14 27/03/2013: http://es.wikipedia.org/wiki/Cookie_(inform%C3%A1tica)

Enlace 9: “Sesiones en PHP II”, Rubén Alvarez, 01/01/2011: http://www.desarrolloweb.com/articulos/321.php

Enlace 10: “Cross Site Request Forgery – Wikipedia, la enciclopedia libre”, última modificación 21:51 13/03/2013: http://es.wikipedia.org/wiki/Cross_Site_Request_Forgery